Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 20819

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2022.

Fifth Semester

Computer Science and Engineering

MA 8551 — ALGEBRA AND NUMBER THEORY

(Common to Computer and Communication Engineering/Information Technology)

(Regulations 2017)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Define Cyclic group and find all the generators of $(\mathbb{Z}_{18}, \oplus)$.
2. Determine all the units of Gaussian integer $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$
3. Check whether the polynomial x^4+2x+2 is irreducible or not over the field of rational.
4. Define irreducible polynomial with example
5. Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7.
6. Evaluate $1011_{two} \times 101_{two}$.
7. Determine whether the LDEs : $12x+18y=30, 2x+3y=4$, and $6x+8y=25$ are solvable.
8. Find the remainder when 16^{53} is divided by 7.
9. Computer : $\phi(16)$ and $\phi(28)$.
10. Solve the linear congruence. $25x \equiv 13 \pmod{18}$.

PART B — (5 × 16 = 80 marks)

11. (a) (i) State and prove Lagrange's theorem. Use Lagrange' theorem to show that an group of prime order is cyclic. (12)

(ii) If G be a finite group of order pq where p and q are primes with $p > q$. Then G has at most one subgroup of order p. (4)

Or

(b) (i) Show that every finite integral domain is a field. (8)

(ii) Let $f : R \to R'$ be an onto ring homomorphism and $K = Ker(f) = \{x \in R \mid f(x) = 0\}$. Then show that $\frac{R}{K}$ is isomorphic to R'. (8)

12. (a) (i) State and prove Unique Factorisation theorem for polynomial rings. (10)

(ii) Show that if a polynomial $f(x)$ is divided by $(x-a)$, then $f(a)$ is the remainder. (6)

Or

(b) (i) Show that if R is an integral domain than $R[x]$ is also an integral domain. (6)

(ii) Let $f(x) = 2x^4 + 3x^3 - 5x^2 - 3x + 1$ and $g(x) = 7x^4 - 5x^3 + 2x^2 - x + 11$. Compute $f(x) + g(x)$ and $f(x) \cdot g(x)$ in the following ring

(1) $\mathbb{Q}[x]$

(2) $\mathbb{Z}_7[x]$

(3) $\mathbb{Z}_2[x]$

(4) $\mathbb{Z}_{11}[x]$ (2+3+3+2=10)

13. (a) (i) State and Prove division algorithm. (8)

(ii) Show that the GCD of the positive integers a and b is a linear combination of a and b. (8)

Or

(b) (i) Explain Euclidean algorithm and Using the Euclidean algorithm, express GCD(2076, 1776) as a linear combination of 2076 and 1776. (8)

(ii) State and prove fundamental theorem of arithmetic. Using this to find the canonical decomposition of 2520. (8)

14. (a) (i) Solve the LDE $1076x + 2076y = 3076$ by Euler's method. (8)

(ii) Find the general solution of the LDEs : $12x + 30y - 42z = 66$ and $6x + 12y - 15x = 33$. (8)

Or

(b) (i) Find the positive integers n for which $\sum_{k=1}^{n} k!$ is a square. (8)

(ii) State the Chinese Remainder Theorern(CRT) and Using CRT to solve the system $x \equiv 1(\text{mod } 2), x \equiv 2(\text{mod } 3), x \equiv 3(\text{mod } 5)$. (8)

15. (a) (i) State and prove Wilson theorem. Using this theorem to show that $\frac{(np)!}{n!\,p^n} \equiv (-1)^n \pmod{p}$, where p is prime and n is any positive integer. (8)

(ii) State and prove Fermat's theorem and using this theorem to find the remainder when 24^{1947} divided by 17. (8)

Or

(b) (i) Prove that $\varphi(p^n) = p^n - p^{n-1}$, where $n \geq 1$. (8)

(ii) Prove that, if p and q are distinct prime, then $p^{q-1} + q^{p-1} \equiv 1(\text{mod } pq)$. (8)
